Avaya™ Interactive Response
Release 2.0
Security

Issue 1.0
Publication Date: April 2006

Notice
While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer
Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer
Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty
Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the Avaya Support Web site:

http://www.avaya.com/support

License
USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)
Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Shrinkwrap License (SR). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Third-party Components" for more information).

Copyright
Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:

http://support.avaya.com/ThirdPartyLicense/

Preventing toll fraud
"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention
If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site:

http://www.avaya.com/support

Providing Telecommunications Security
Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that can be accessed by this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who might be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions might be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there might be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it might result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security
The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers must carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities
Customers might experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance
Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment is the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. might void the user's authority to operate this equipment.

Federal Communications Commission Statement

Part 15:

Note:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canadian Department of Communications (DOC) Interference Information
This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Europeénne) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the Avaya Support Web site:

http://www.avaya.com/support

Trademarks
Avaya, the Avaya logo, and Interaction Reponse, are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support Web site:

http://www.avaya.com/support

Avaya support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1 800 242 2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site:

http://www.avaya.com/support

Contents

Security overview

In today's computing world, security is an ever-increasing concern to system administrators. Avaya is keenly aware of security issues and has worked hard to help make sure its systems are as secure as possible.

Toward that end, we have prepared a white paper to help guide you in making security policy decisions concerning your Avaya IR system. We strongly encourage you to read and implement the recommendations in the white paper, *Avaya™ Interactive Response Security* collections/print_Security_White_Paper.pdf.

The rest of this section provides additional information regarding system security.

This section includes the following topics:

Security enhancements in Release 2.0

The following is a summary of the security enhancements introduced in Avaya Interactive Response Release 2.0:

- **Use of Solaris 10 as an Operating System (OS)**

  The use of Solaris 10 as an OS provides additional security enhancements like password encryption, a cryptographic framework for data security, and improved user rights management. The use of Secure Shell (SSH) on Solaris 10 provides you with the ability to run Secure File Transfer Protocol (SFTP) service. The SFTP service is similar to File transfer Protocol (FTP), but performs all operations over an encrypted SSH transport link, thus gaining the features of public key encryption and compression. SSH is a secure replacement for Telnet, rlogin, rcp, rsh and provides secured TCP tunnels.

The SFTP service, in the context of Avaya IVR Designer 5.3 implements the client part of the SSH protocol, On IR systems using Solaris 10 as the operating system, SSH is provided by default. On IR systems using Solaris 8 as the operating system, SSH can be installed using the openSSH package (www.sunfreeware.com). Avaya IVR Designer Release 5.3 offers the option of using either FTP or SFTP.

A common misconception about SFTP is that SFTP is simply FTP run over SSH. However, SFTP is the service, which works above the SSH protocol. SFTP expects the underlying SSH protocol to secure authentication and security. Therefore, SFTP is most often associated with SSH. Compared to the earlier Secure Copy protocol (SCP), the SFTP protocol allows for many more operations on remote files, and functions like a remote file system protocol. SFTP also provides a more secure connection, as against using FTP or telnet because passwords are never transferred in clear text, preventing the possibility of capture of sensitive data, while eavesdropping on the connection. Data is also encrypted during the transfer, making it difficult to spy or modify the connection

- **JDBC connection supporting encryption**

  The JDBC connection provides connectivity between the Avaya IR server and remote database servers. The JDBC connection supports connections for up to five different databases. Each database is accessed using a Data Interface Process (DIP) that has been configured with the appropriate administration information for that database. For IR R2.0, after configuring administration information, the provision has been introduced for you to store your database password in an encrypted format.

- **Encryption of VOIP signaling and media streams**

  The encryption of VOIP media and signaling streams provides security to VOIP traffic transmitted between the IR and the MultiVantage switch, as well as any routers or other equipment that transmit IP traffic between the IR and the MultiVantage switch. This reduces the risk of eavesdropping and increases security for sensitive applications or data.

- **Backup and Restore using a Tape Drive**

  For IR R2.0, tape backup mechanism has been introduced, in addition to NFS (Network File System) backup already present. This enhancement provides you with increased data security.

- **Disabling of unneeded network services**

  For customers who purchase the complete Avaya IR system solution (that is, both the hardware and software), unneeded network services are disabled by default.

  Customers who purchase the software-only solution can, if they wish, make their systems conform to these standards by running the *disableServices* utility on page 10. They may also consult the white paper, *Avaya™ Interactive Response Security* collections/print_Security_White_Paper.pdf and follow the recommendations in that publication.

Note:
The disabling of network services towards heightened system security began with Release 1.2

- **The Avaya™ Interactive Response Security white paper**

  To help you further protect your system, we have produced a white paper that details the steps and measures you can take to enhance the security of your system. We strongly recommend that you read and implement the practices described in the white paper, *Avaya™ Interactive Response Security* collections/print_Security_White_Paper.pdf.

Securing access to the system

For good security, you should restrict system access to authorized personnel. There are two types of access:

- Physical access
- Operational and administrative access

Following are some considerations regarding the restriction of access to the system.

Physical access

To restrict physical access to the system, the system should be located in a secured location that can only be reached by authorized personnel.

Operational and administrative access

To restrict operational and administrative access to the system, the Avaya IR system uses both the built-in capabilities of the Solaris operating system and the ASG Security feature.

For information about securing the operating system and securing other parts of the system using Solaris, see "Managing System Security Topics" in *Solaris System Administration Guide, Volume 2*. These documents are available in *Avaya IR System Help* (under "Print documents") or from the Sun Web site (http://www.sun.com).

Securing the network

Any server that is connected to the Internet is potentially subject to unauthorized use and malicious attacks. Like any other server on your network, the Avaya IR system can and should be configured in accordance with your own corporate security policies.

This section describes approaches that Avaya recommends for securing the network.

Using a firewall

Avaya strongly recommends using a firewall product to protect your internal LAN, including any Avaya IR servers, from unauthorized access. Firewalls sit between your LAN and the Internet and control access to designated ports. Most firewalls can be configured to allow specified remote IP addresses to connect to designated ports.

For information about establishing a firewall on your network, see the following resources:

- "Network Security" in *Solaris System Administration Guide, Volume 2*. These documents are available in *Avaya IR System Help* (under "Print documents") or from the Sun Web site (http://www.sun.com).
- Customer documentation for your network equipment

If using a firewall is not an option, you can to configure your Avaya IR system on a physically isolated LAN. For more information see Physically isolating the LAN on page 10.

Disabling unused network services

Network services are a frequent target of unauthorized access attempts. Any network service that is enabled may provide a potential mechanism for an unauthorized connection to be made to the system. For this reason, we recommend that you disable any network services not needed by the Avaya IR system. These services are disabled by default on complete system (hardware and software) solutions. For software-only solution systems, you can run the disableServices on page 10 utility to match the complete system configuration.

If any of these services are needed in your operating environment, you can enable them.

Note:
The disabling of network services does not remove the need for a firewall.

For more information and recommendations about enabling and disabling network services, see the document *Avaya™ Interactive Response Security* collections/print_Security_White_Paper.pdf. Also see *Solaris System Administration Guide, Volume 3.* These documents are available in *Avaya IR System Help* (under "Print documents") or from the Sun Web site (http://www.sun.com).

Disabling the telnet feature

The telnet service provides you with a mechanism to connect to a host machine from a remote system. The telnet service is not needed for IR operation. Avaya recommends you disable the telnet feature on a software-only IR solution.

Note:

Companies should not disable the telnet service unless they have another means of accessing the system, such as using the system console or Secure Shell

Running the disableServices utility

Avaya has provided a utility to disable unneeded network services and help harden system security. This is intended especially for those customers who purchase the Avaya IR software-only solution, but it can be used at any time to set the system to the default and preferred settings for network services. Running this utility will ensure that your system conforms to the same standards as the Avaya IR complete system solution at time of purchase.

Note:

For more information about and recommendations on disabling and enabling network services in Avaya IR systems, see the white paper, A*vaya™ Interactive Response Security* collections/print_Security_White_Paper.pdf.

To run the *disableServices* utility:

1. Log in as root if you are not already logged in.
2. At the system prompt, enter **/vs/bin/util/disableServices**

   The utility runs and sets all network services to the same state used by the complete system solution. It also generates a list of all the network services that it disabled and stores the list in the file **/voice1/disabledServices.log**.

Physically isolating the LAN

As an alternative to using a firewall, you can protect your Avaya IR system by configuring it on a LAN that has no physical connection to the Internet. Sometimes referred to as an "island LAN," this type of network environment has its own LAN switch and contains only those network elements with which the Avaya IR system needs to interface, such as speech servers, database servers, a backup server, and a Multivantage system (for VoIP connectivity and ASAI feature functionality). Because this LAN has no physical connection to the internet, there is no need to use a firewall to protect the system from unauthorized access.

If you cannot isolate the LAN, Avaya recommends using a firewall to protect your system. For more information, see Using a firewall on page 9.

Restricting administration permissions

Administration of Avaya software can be restricted by assigning permissions to users, as described in the following table:

Permission	Description
Root	The user can perform any task on the system
Administration	The user has full control of the voice system and features through Web Administration and the command line
Operations	The user has access to configuration management, reports, administration, and system monitor capabilities, but does not have control of the voice system. Note that the system monitor is only administrable through the command line.

Logging in as root

For security purposes, the Avaya IR system is setup by default to restrict access of the **root** account to users logging in from the console. Users are not allowed to log in as root remotely (using telnet, for example). It is possible, however, to log in remotely as another user and then switch to root using the **su** command.

Although we strongly recommend against doing so, you can also change the default settings on the system to allow remote login as root.

To allow remote login as root:

1. Log in as root.

   You must do this using the console or by logging in as another user then entering **su root** and the root password.

2. Enter **cd /etc/default**

3. Enter **vi login**

   The login file opens in the vi editor.

4. Using the vi editing commands, find the following line:

   CONSOLE=/dev/console

5. Comment the line by inserting **#** at the beginning of the line.

6. Save and close the file.

For more information about root and the **su** command, see *Solaris System Administration Guide, Volume 1.* These documents are available in *Avaya IR System Help* (under "Print documents") or from the Sun Web site (http://www.sun.com).

Index